Defense Information Systems Agency

A Combat Support Agency

DoD DMZ

Dan Gahafer
DISA CD4 Division Chief
April 2009

DISA
A Combat Support Agency

Agenda

- **DoD DMZ Overview**
  - **CSD DMZ Today**
  - **NIPRNet DoD DMZs**
- **OSD/NII Guidance**
- **Summary**

DISA
A Combat Support Agency

Overview

- **Protect Internet-facing apps & services:**
  - **Web**
  - **E-mail**
  - **FTP**
- **Filter outbound web requests/inbound content**
- **Secure DNS infrastructure**
  - **Situational awareness**
  - **Inbound queries**
  - **Outbound queries**
  - **DNSSEC**

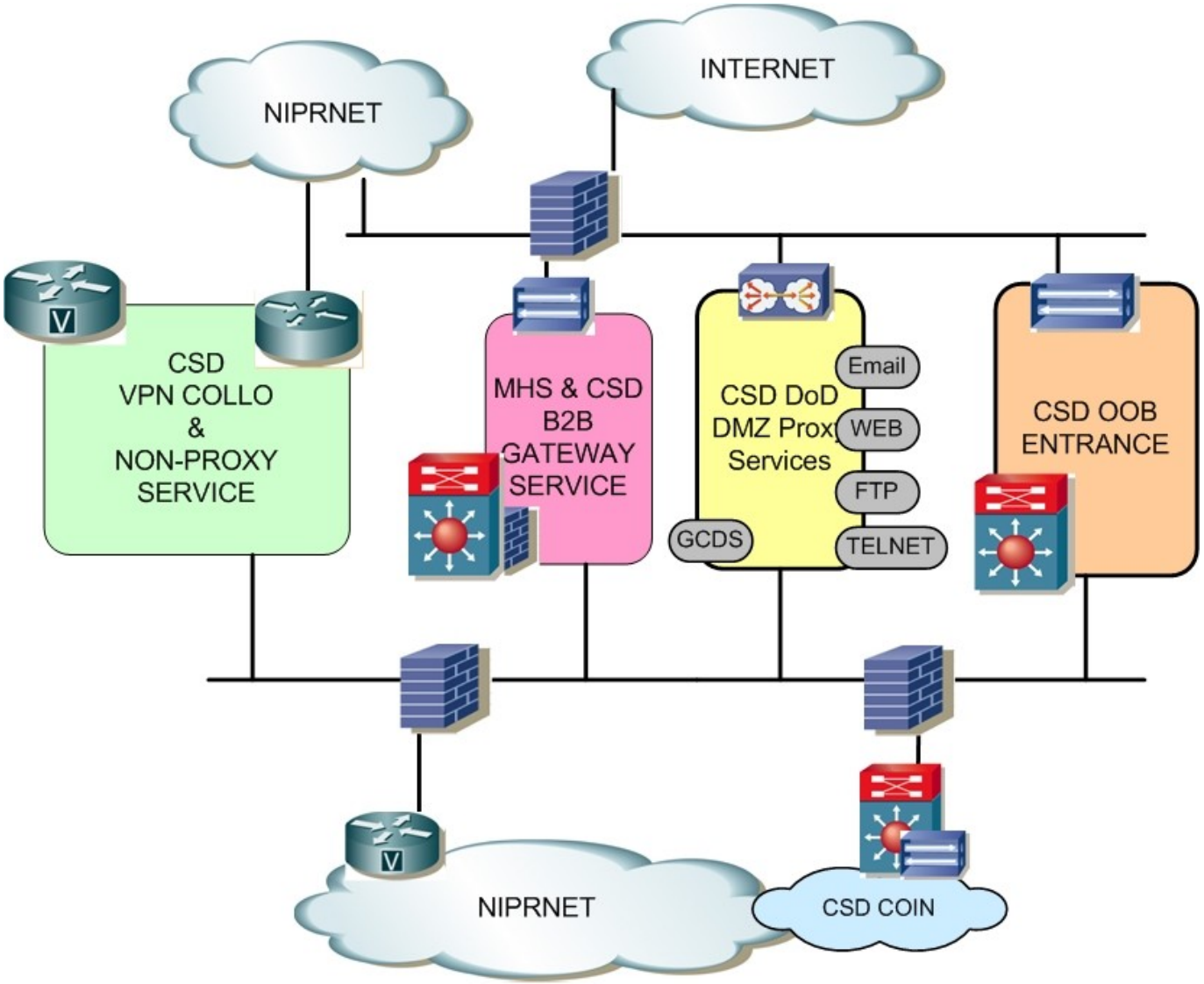
DISA
A Combat Support Agency

CSD DMZ Today

- **Designed and Operated by CSD since 2001**
- **Four locations with two additional being deployed**
  - **Columbus, San Antonio, Montgomery and Ogden**
  - **Future sites in Mechanicsburg and Oklahoma City**
- **Current DMZ services**
  - **Services include**
    - **Proxy Services (Web, FTP, Telnet, Email, GCDS)**
    - **MHS and CSD Business To Business (B2B) Gateway Service**
    - **CSD Out-of-band (OOB) Entrance**
    - **CSD IA Architecture Non-Proxy Path**
    - **CSD VPN Collocation Services**

DISA
A Combat Support Agency

CSD DMZ Today



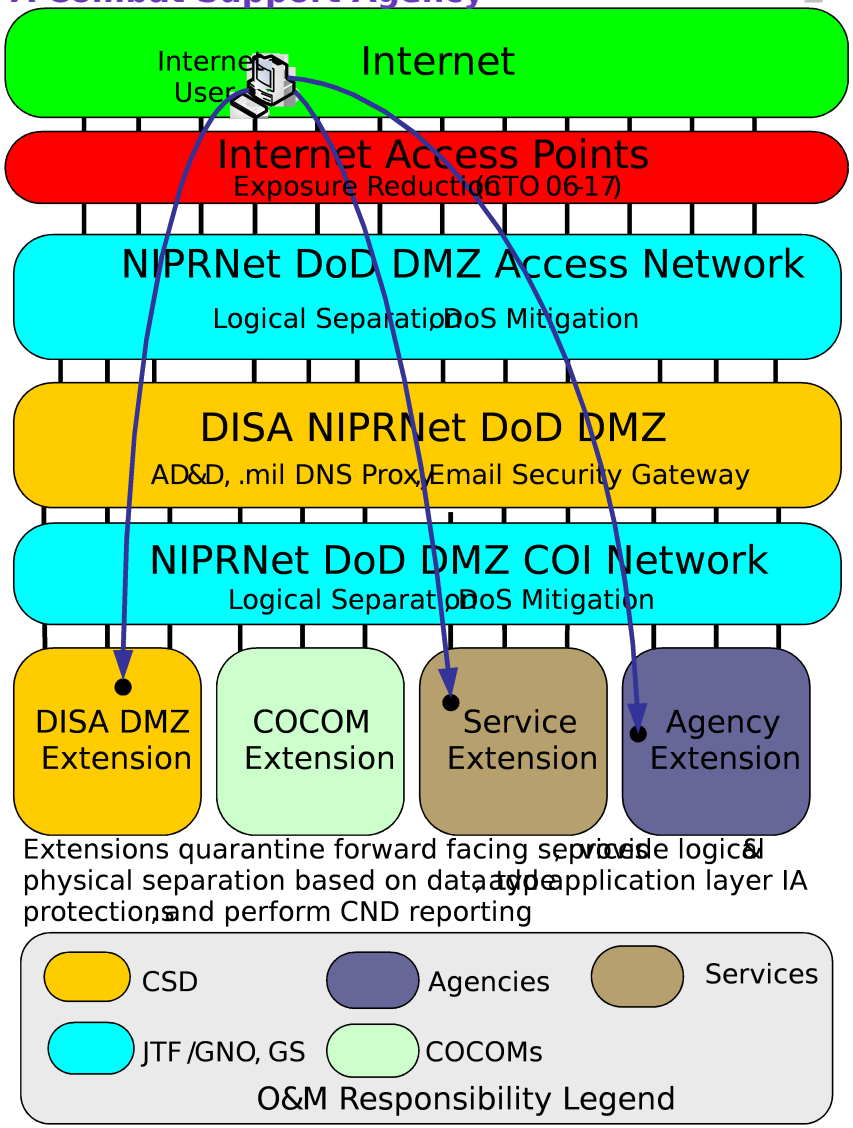
DISA
A Combat Support Agency

DoD DMZ Guidance

- **OSD Tasking**
  - **Develop Engineering Plan that includes Operational, System, and Technical planning for implementing "robust protective measures at the NIPRNet perimeter…"**
    - **Consolidate, consistently manage, and control public access and visibility to all DoD assets and information.**
    - **Consider recommendations by the GIG IA Architecture Office**
- **JTF-GNO Tasking**
  - **Logically or physically group publicly accessible DoD NIPRNet servers (including but not limited to DNS, Web, and Email) to prevent adversaries' network reconnaissance, exploitation and attack activities.**

DoD DMZ Target Architecture

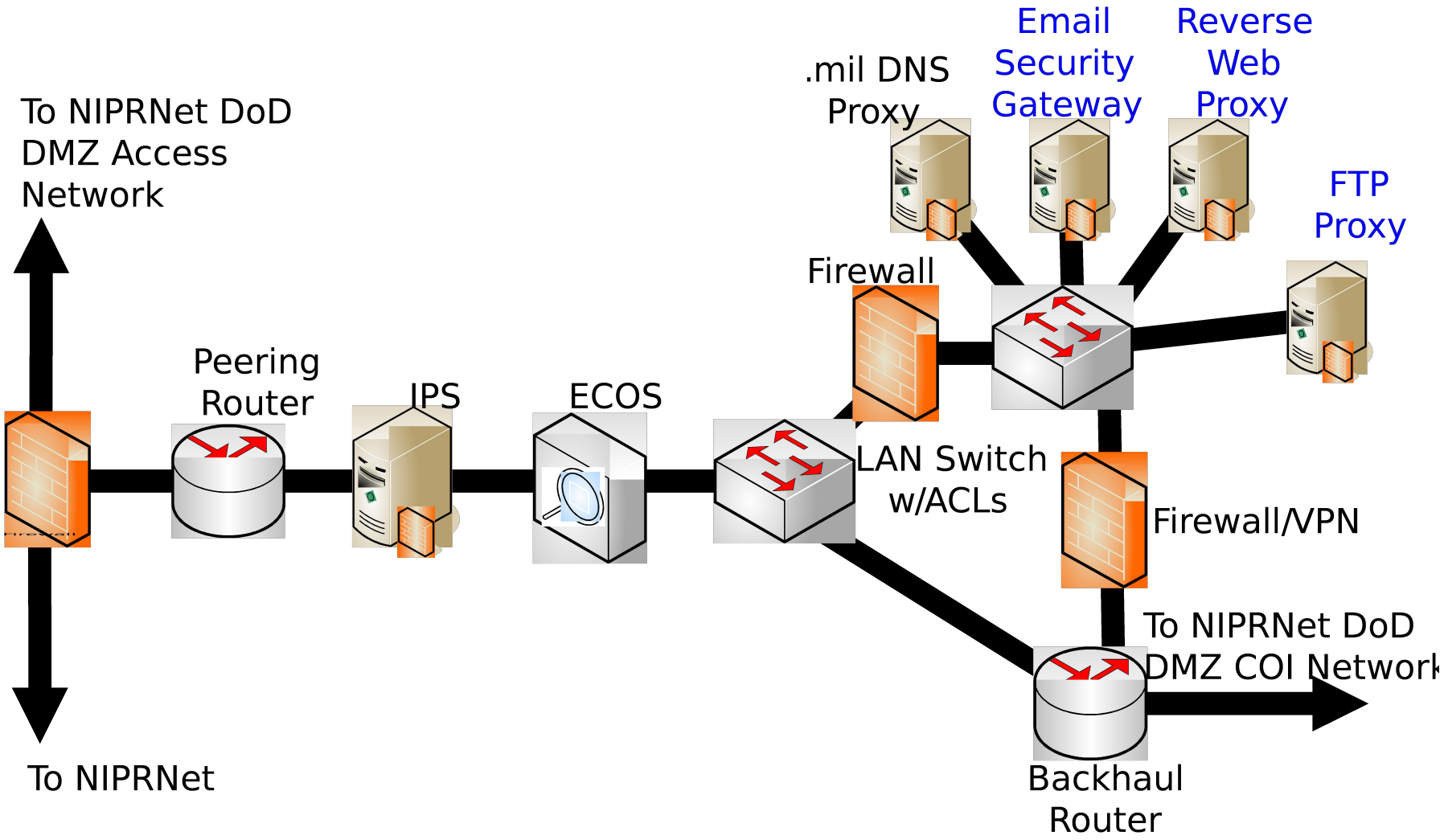
A Combat Support Agency



- DoD DMZ is comprised of the Front Ends and Extensions
- Applications can physically remain at the CC/S/A location, in a DMZ Extension
- DoD DMZ Access and COI networks *logically* connect the DMZ components and stage the Internet facing applications at the Internet/NIPRNet boundary
- All inbound connections traverse the NIPRNet DoD DMZ Front Ends

DISA
A Combat Support Agency

Target Front End

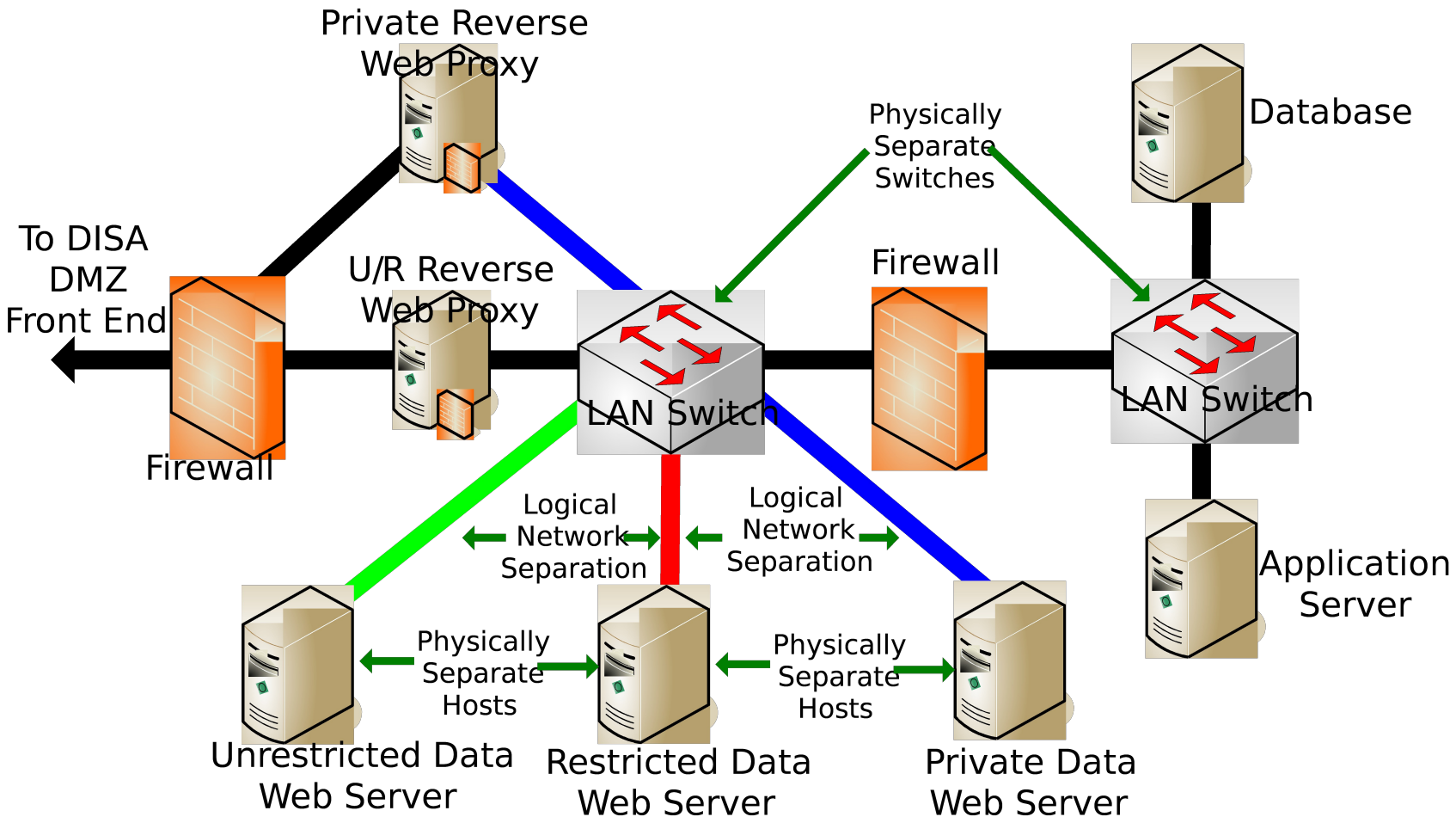


NOTE: Capabilities in Blue Lettering can be used by CSS/As

DISA
A Combat Support Agency

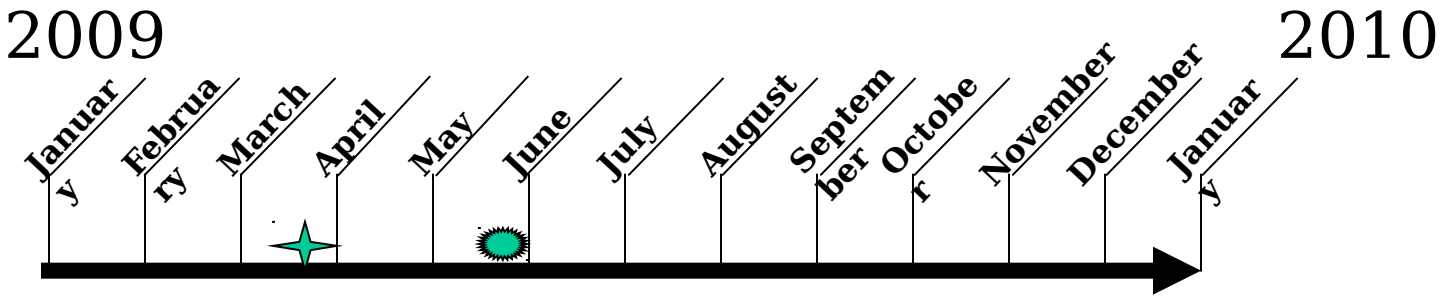
DoD DMZ Extension

Near Term Separation Requirements are Relaxed



Deployment Timeline (2009)

ITEMS IN RED INDICATE ACTIONS THAT IMMEDATELY INCREASE THE IA POSTURE OF THE NIPRNET



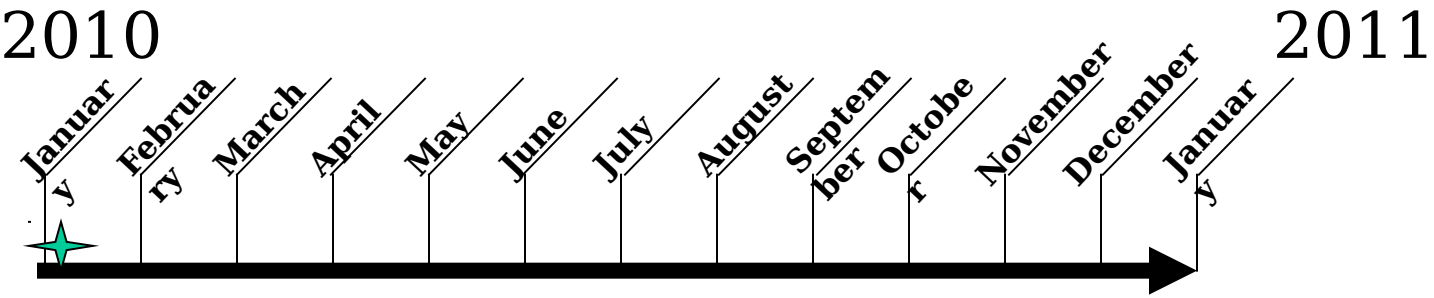
.mil DNS Proxy Filters will be modified to allow inbound traffic HTTP, FTP, SMTP, and DNS

DMZ Extensions (Installed) CC/S/As implement initial set of logical / physical separation requirements

Implement NIPRNet DoD DMZ Access Network

Deployment Timeline (2010)

ITEMS IN RED INDICATE ACTIONS THAT IMMEDATELY INCREASE THE IA POSTURE OF THE NIPRNET



STIG physical and logical separation requirements become enforceable

Enhance DMZs with VPN Capability*

2010/2011 Items not scheduled:

- **Begin connecting NIPRNet DoD DMZ Extensions to NIPRNet DoD DMZ Front Ends (via VPN)**
- **Enhance DMZs with Log Aggregation**
- **Enhance DMZs with Intrusion Prevention System**
- **Enhance DMZs with ECOS**

*** VPN Capability will provide logical network isolation of traffic flows between NIPRNet DoD DMZ and NIPRNet DoD DMZ extensions (Logically isolated from NIPRNet). Network isolation may be implemented using IPSec or MPLS.**

DISA
A Combat Support Agency

Summary

- **NIPRNet DoD DMZs are located in DISA DECCs**
- **CSD DMZs are collocated with NIPRNet DoD DMZs and provide several proxy services for DISA customers**
- **All DECC Unclassified production enclaves are front-ended by both DoD DMZs and CSD DMZs**
  - **Internet accesses traverse both**
  - **NIPRnet accesses traverse only the CSD DMZs**
- **Application separation issues remain to be resolved**

DEFENSE INFORMATION SYSTEMS AGENCY